

Amplifying the randomness of weak sources correlated with devices

H. Wojewódka,^{1,2} F. Brandão,^{3,4} A. Grudka,^{1,5} M. Horodecki,^{1,2}
K. Horodecki,^{1,6} P. Horodecki,^{1,7} M. Pawłowski,^{1,2} and R. Ramanathan^{1,2}

¹ National Quantum Information Centre of Gdańsk

² Institute of Theoretical Physics and Astrophysics, Gdańsk University

³ Quantum Architectures and Computation Group, Microsoft Research, Redmond, WA

⁴ Department of Computer Science, University College London WC1E 6BT, United Kingdom

⁵ Faculty of Physics, Adam Mickiewicz University

⁶ Institute of Informatics, Gdańsk University

⁷ Faculty of Applied Physics and Mathematics, Technical University of Gdańsk

(Dated: January 26, 2016)

The problem of device-independent randomness amplification against no-signaling adversaries has so far been studied under the assumption that the weak source of randomness is uncorrelated with the (quantum) devices used in the amplification procedure. In this work, we relax this assumption, and reconsider the original protocol of Colbeck and Renner [4] on randomness amplification using a Santha-Vazirani (SV) source. To do so, we introduce an SV-like condition for devices, namely that any string of SV source bits remains weakly random conditioned upon any other bit string from the same SV source and the outputs obtained when this further string is input into the devices. Assuming this condition, we show that a quantum device using a singlet state to violate the chained Bell inequalities leads to full randomness in the asymptotic scenario of a large number of settings, for a restricted set of SV sources (with $0 \leq \varepsilon < \frac{(2^{(1/12)} - 1)}{2(2^{(1/12)} + 1)} \approx 0.0144$). We also study a device-independent protocol that allows for correlations between the sequence of boxes used in the protocol and the SV source bits used to choose the particular box from whose output the randomness is obtained. Assuming the SV-like condition for devices, we show that the honest parties can achieve amplification of the weak source against this attack for the parameter range $0 \leq \varepsilon < 0.0132$. We leave the case of a yet more general attack on the amplification protocol as an interesting open problem.

Introduction

In many applications, like numerical simulations, cryptography or gambling, just to name a few, free randomness is desired due to the fact that a wide range of results is based on it. In practice, however, random sources are rarely private and only weak partially sources of randomness are available. That is why the problem of randomness amplification became useful and worth investigating. Overall, the idea is to use the inputs from a partially random source and obtain perfectly random output bits. In classical information theory, randomness amplification from a single weak source is unattainable ([16]). However, it becomes possible, if the no-signaling principle is assumed and quantum-mechanical correlations are used. Such correlations are revealed operationally through the violation of Bell inequalities.

As a weak source to be amplified, we consider an ε -SV source (named for Santha and Vazirani [16]), where ε is a parameter which indicates how far we are from full randomness. An ε -SV source is given by a probability distribution $P(\varphi_1, \dots, \varphi_n, \dots)$ over bit strings such that

$$\begin{aligned} (0.5 - \varepsilon) &\leq P(\varphi_1|e) \leq (0.5 + \varepsilon), \\ (0.5 - \varepsilon) &\leq P(\varphi_{i+1}|\varphi_1, \dots, \varphi_i, e) \leq (0.5 + \varepsilon) \quad \text{for every } 1 \leq i \leq n, \end{aligned} \tag{1}$$

where the e represents an arbitrary random variable prior to φ_1 , which can influence $\varphi_1, \dots, \varphi_n, \dots$. Note that, when $\varepsilon = 0$, bits are fully random, while they are fully determinis-

tic when $\varepsilon = 0.5$. For brevity, throughout the rest of the paper we will write p_- for $(0.5 - \varepsilon)$ and p_+ for $(0.5 + \varepsilon)$.

In the research on randomness amplification, the paper of Colbeck and Renner [4] is certainly crucial. It is also a starting point for our idea. The authors consider the bipartite scenario of the chained Bell inequality and prove that, under certain assumptions (discussed later), it is possible to amplify randomness of ε -SV sources, provided $\varepsilon < (\sqrt{2} - 1)^2 / 2 \approx 0.086$. The result may be improved, as is done in [12]. There, based on the observation that extremal points of the set of probability distributions from an ε -SV source are certain permutations of Bernoulli distributions with parameter $(0.5 - \varepsilon)$, randomness amplification was obtained for any $\varepsilon < 0.0961$. Moreover, the bound was shown to be tight, which means that under these assumptions, it is not possible to achieve randomness amplification using the chained Bell inequality above this threshold.

Gallego et al. [5] show that, given an ε -SV source, with any $0 < \varepsilon < 0.5$, and assuming no-signaling, full randomness may be certified using quantum non-local correlations. In this paper, the Bell scenario of five-party Mermin inequality is considered, however, unlike in the protocol proposed in [4], the hashing function used to compute the final random bit is not explicitly provided and a large number of space-like separated devices is required.

Further results were obtained in [6], [8], [7], [9] etc., a wide range of protocols have been proposed, these are summarized and compared in Table I in [7]. The problem has been considered from different points of view and a lot of obstacles, such as the requirement of an infinite number of devices or no tolerance for noise, have already been overcome. However, relaxing the assumption about independence between a source and a device has not yet been widely studied, especially in the context of a finite device framework against a no-signaling adversary.

In this paper, we relax this assumption, i.e., do not require a source and a device to be independent, while still considering a finite device protocol for amplification against a no-signaling adversary. Instead, we only limit the correlations between the source and device by one constraint, which we call the SV-condition for boxes and specify in detail later. We prove explicitly that the most malicious correlations (between a source and a device) are not allowed due to the assumption that an ε -SV source remains an ε -SV source even upon obtaining the inputs and outputs from boxes (SV-condition for boxes). Hence, randomness amplification is still possible. Our new method of proof allows to analyze an attack where an adversary sends to the honest parties those boxes that are particularly adapted to their measurement settings. We explain the dangers of such attacks with an explicit example in Section 2.

So far, only Chung et al. [8] have tried to weaken the independence assumption, however their approach to this question explicitly requires the use of a large number of devices which is a major drawback we desire to avoid. We therefore propose an alternative approach to the problem. We believe that these results give a new insight into the problem and, due to the clarity of assumptions, will also be significant in the more general task of obtaining secure key bits in cryptography. Moreover, as we shall see, in the present paper, we also obtain randomness under weaker assumptions than those of [8].

The paper is organized as follows. In Section I we introduce some basic notations and definitions. A motivation for the paper is described in Section II with a toy example of an attack strategy for the adversary. In Section III we formally state the assumptions in the paper and discuss the results for a single no-signaling box. Section IV is devoted to the explicit example of the chained Bell inequality, which is interesting because it may be compared with the results of Colbeck and Renner [4]. In Section V we revisit the Colbeck and Renner protocol for amplification of randomness using the chained Bell inequality. We then prove, in Section VI, that under the relaxed assumption, against a general symmetric attack, the protocol allows for amplification in the parameter range $0 \leq \varepsilon < 0.0132$. The final part of the paper, in which we certify randomness does not finalize the problem yet. Although the intuition is that we analyze the strongest possible

attack, the symmetry assumption should formally be relaxed. The aim of further research is to investigate whether stronger attacks than the one proposed in this paper are possible, and if so whether a protocol can be devised to achieve amplification against these as well.

I. PRELIMINARIES

A. No-signaling boxes

In our study we use a family of probability distributions, usually called a box, denoted by $P(O|I)$, where I and O are random variables describing the vectors of inputs and outputs, respectively.

To talk about randomness amplification, it is advisable to explain what is meant by the no-signaling condition. In the simplest case, when there are only two parties: Alice and Bob, the no-signaling assumption is that

$$\begin{aligned} \sum_y P(O = (x, y) | I = (u, v)) &= \sum_y P(O = (x, y) | I = (u, v')) \quad \text{for every } u, v, v', x, \\ \sum_x P(O = (x, y) | I = (u, v)) &= \sum_x P(O = (x, y) | I = (u', v)) \quad \text{for every } u, u', v, y. \end{aligned} \quad (2)$$

B. Bell values observed in laboratories

Theoretically, there may exist no-signaling boxes which attain the algebraic violation of chosen Bell inequality. However, as for now, we are able to use in laboratories only these boxes which violate the inequality up to the value obtained within the rules of quantum mechanics. This simply means that the Bell value observed in a lab may not be lower (here a larger violation is characterized by a smaller value for the Bell expression) than the value predicted by quantum mechanics.

C. Bell inequalities useful for randomness amplification

It is well-known that quantum mechanics allows for non-local correlations between spatially separated systems. Occurrence of such correlations can be verified through the violation of Bell inequalities. The convex set formed by the correlations described by quantum theory is sandwiched between the sets of classical and general no-signaling correlations. Only extremal boxes (vertices) of the no-signaling polytope are completely uncorrelated with the environment and hence provide intrinsic certified randomness. It has been recently proven in [15] that non-local vertices of the no-signaling polytopes of correlations admit no quantum realization. For amplification of SV sources, Bell inequalities with the property that the optimal quantum value equals the optimal no-signaling value are required. For such Bell inequalities (e.g. GHZ paradoxes [11], pseudo-telepathy games [10] or Bell inequalities for graph states [13]) or those where the quantum violation is close to algebraic (such as the chained Bell inequality [2]) the quantum set reaches the corresponding facet of the no-signaling polytope.

In this paper we mainly focus on the chained Bell inequality, which has already been used in the research on randomness and privacy amplification (see [4], [12] or [1]).

II. MOTIVATION AND A TOY EXAMPLE

We now exemplify a possible attack that utilizes correlations between a weak source and device in the simplest scenario of boxes with binary inputs and outputs. Even though these boxes do not constitute a resource for randomness amplification, the attack can already be described in terms of these.

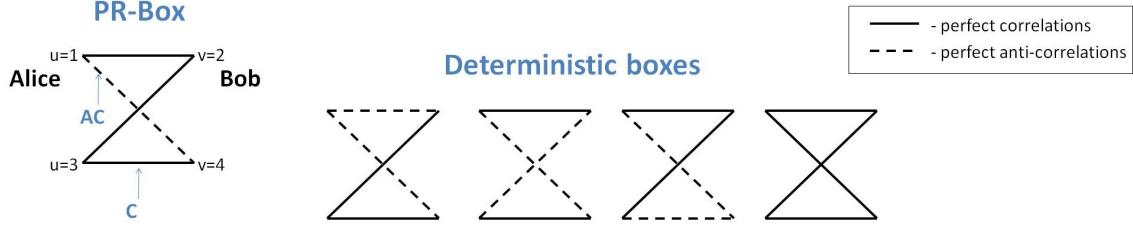


FIG. 1: Examples of bipartite boxes with binary inputs and outputs denoted by graphs. The Popescu-Rohrlich box (on the left) and local (deterministic) boxes (on the right).

Imagine that Alice and Bob share a box L which is a mixture of local boxes L_{ij} where $i = 1, 3$ label Alice's inputs and $j = 2, 4$ label Bob's inputs:

$$L = \frac{1}{4} (L_{12} + L_{32} + L_{34} + L_{14}). \quad (3)$$

(See Fig. 1 where the PR box and local deterministic boxes are presented and Fig. 2, where the boxes L_{ij} are given explicitly). The bits from an ε -SV source are perfectly correlated to local boxes as

$$P(L_{ij}|S = (k, l)) = \delta_{ik;jl} = \begin{cases} 1, & i = k \text{ \& } j = l, \\ 0, & \text{otherwise,} \end{cases} \quad (4)$$

where S is the random variable describing bits from an ε -SV source.

In the protocols proposed so far such as [4], [12], it is demanded that I and S are perfectly correlated, i.e.

$$P(I = (u, v)|S = (k, l)) = \delta_{uk;vl} = \begin{cases} 1, & u = k \text{ \& } v = l, \\ 0, & \text{otherwise,} \end{cases} \quad (5)$$

which means that bits from the ε -SV source are used as inputs to the box. All the correlations are indicated in Fig. 2. Now, we see that although the box L is manifestly local, the honest parties do not detect it in the protocols proposed so far. Indeed, correlations (4) and (5) imply that input $I = (k, l)$ may only be introduced to box L_{kl} , adapted exactly to this input, so that L mimics the action of the PR box on any input. On the other hand, if there was independence between the ε -SV source and the boxes, the parties would recognize that the object L is local.

To conclude, this toy example clearly illustrates that perfect correlation of inputs and devices excludes any possibility of randomness amplification. To circumvent this type of attack, we introduce the SV-condition for boxes, which is the weakest assumption (thus far) that still allows for randomness amplification.

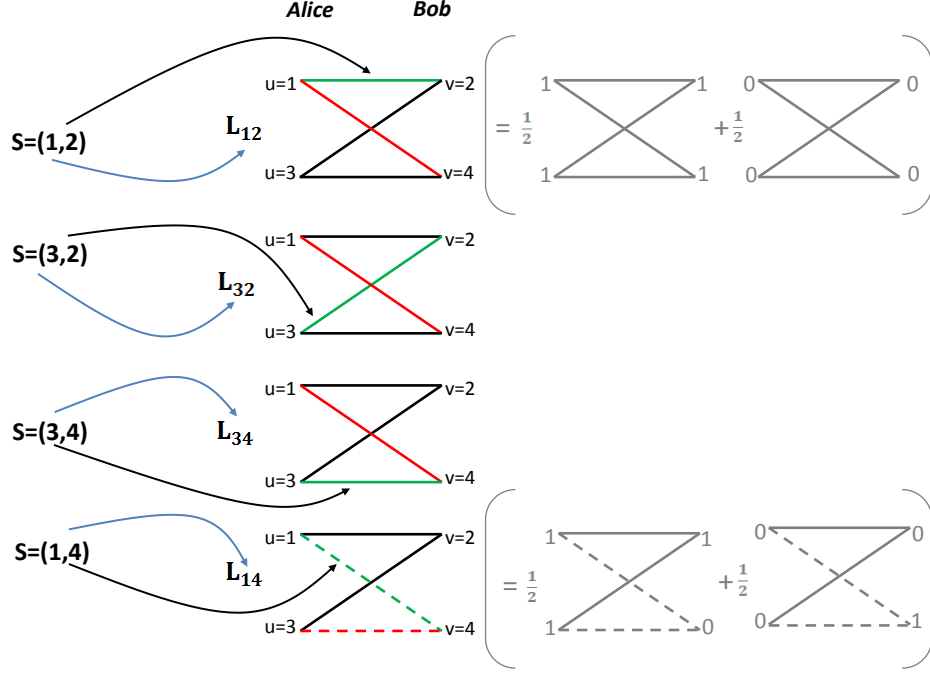


FIG. 2: Bits from an ε -SV source (on the left) are perfectly correlated with local boxes supplied to honest parties (on the right). Correlations described by Eq. (4) are indicated by blue arrows. Additionally, bits from an ε -SV source are perfectly correlated with the inputs to boxes (see Eq. (5)), which is indicated by black arrows. These correlations allow only for measuring green edges and hence Alice and Bob always observe an optimal Bell value. If red edges could be measured, the locality of boxes would be detected.

III. RANDOMNESS AMPLIFICATION FOR A SINGLE NO-SIGNALING BOX

A. Correlations between the source and device: boxes determined by source

Let S denote a random variable which describes an arbitrary portion of subsequent bits from an ε -SV source. Recall that we write I and O for variables which describe the inputs and outputs of the device, respectively. Suppose that bits from an ε -SV source are delivered and simultaneously boxes, that are possibly correlated to them, are supplied. Hence, our object of study is

$$P(O|I, S). \quad (6)$$

Note that S determines how the device acts inside (see Fig. 3).

Remark 1. Even if conditional distributions of the form $P(O = o|I = i, S = s)$ are equal for arbitrary o, i, s , joint distributions $P(O = o, I = i, S = s)$ do not have to be the same. This is just a fact which follows from conventional and meaningful way of thinking about any devices.

B. SV-condition for boxes

Let us now precisely state the main assumption used in this paper, which we call the SV-condition for boxes. Recall that S is a variable which describes an arbitrary portion of subsequent

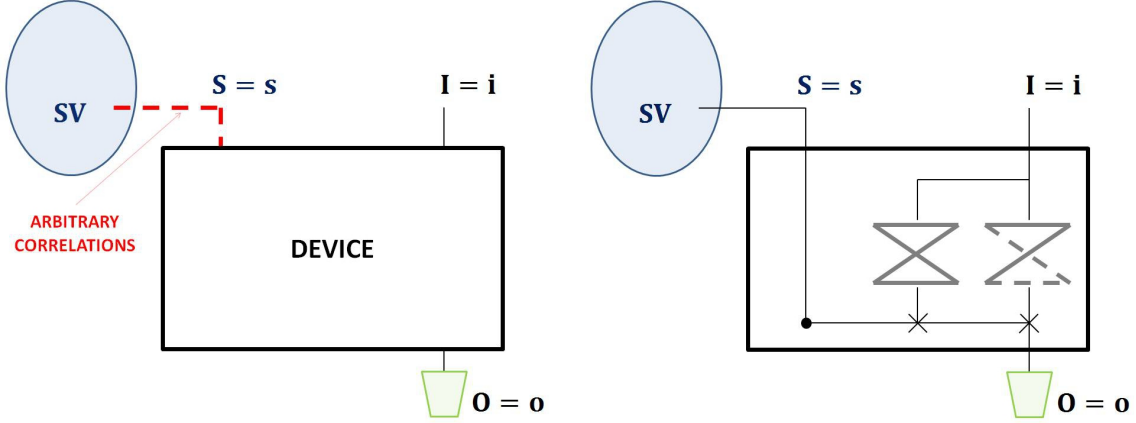


FIG. 3: A priori we allow arbitrary correlations between a source and a box (left). To illustrate how malicious these correlations may be, we recall the example described in Section II (right). Bits from an ε -SV source determine from which box the final output bit is taken. In general, arbitrary input bits may be introduced to the box. The illustration for other Bell inequalities may be much more complicated, but the idea is the same.

bits from an ε -SV source. Now, let S' be a variable describing a disjoint portion of subsequent bits chosen from the same ε -SV source which will be used as the input I to the device. Note that we do not assume any temporal ordering between S and S' . Let $\eta_{\min}, \eta_{\max} \in (0, 1)$ be some functions of $\varepsilon > 0$ and $|I|$ (denoting the number of measurement settings). Although we a priori allow for arbitrary correlations between the source and device, there is one constraint which we impose, namely that if $S' = s'$ is input into the device with $\eta_{\min} \leq P(S = s|S' = s') \leq \eta_{\max}$, then S cannot be guessed perfectly even after knowing the output $O = o$, i.e., for every realization o, s, s'

$$\eta_{\min} \leq P(S = s|O = o, S' = s') \leq \eta_{\max} \quad \text{for } S, S' \text{ such that } \eta_{\min} \leq P(S = s|S' = s') \leq \eta_{\max}. \quad (7)$$

Remark 2. The distribution remains unchanged even if conditioned upon a variable e , which represents some information prior to S' . To avoid unnecessary notation, we neglect it in the condition, since it is irrelevant in what follows.

Assuming condition (7), which we henceforth call the SV-condition for boxes, we certainly assume less than independence between the source and device. Note that the SV-condition for boxes is clearly violated in the toy example from Section II. Indeed, suppose that there are some testers who obtain further bits from the SV source denoted by the variable S' (so that $p_{\min} \leq P(S' = s'|S = s) \leq p_{\max}$ and conversely $\zeta_{\min} \leq P(S = s|S' = s') \leq \zeta_{\max}$ for some $\zeta_{\min}, \zeta_{\max} \in (0, 1)$, whose explicit forms are derived in Appendix I) and input them into the box. When they input $S' = s$ and observe an output that does not mimic the PR box, i.e. $O \neq o_{PR}$, then due to the perfect correlations between S and L_{ij} they know that $S \neq s$, i.e., we have

$$P(S = s|S' = s, O \neq o_{PR}) = 0 \quad (8)$$

which violates Eq. (7).

C. Comparison with assumptions in previous results

Let us now describe how the SV-condition for boxes assumption used in this paper differs from the assumptions in previous results. Firstly, note that as shown by the attack described

in Section II, to retain the possibility of randomness amplification, one has to necessarily make some assumptions on the correlations between the source and the device. The intuition behind the possible assumptions is the following: the SV source should remain the SV source even if conditioned upon any possible event in the universe. In particular, it should remain an SV source when conditioned upon the outputs of any available devices. In other words, if we input a portion of bits from the SV source into a device, then any other portion of bits should still obey the SV source conditions.

A stronger assumption that one may consider, is that for an input to the device that is *independent* of the SV source, when conditioned on the output, the source should remain an SV source. This condition is analogous to a similar condition on min-entropy sources, which is derived from the assumption by Chung, Shi and Wu (CSW) in [8]. Namely, CSW consider a quantum scenario, where the device D and the min-entropy source S are correlated as in the cq-state ρ_{SD} ,

$$\rho_{SD} := \sum_s P(S = s) |s\rangle\langle s| \otimes \rho_s^D \quad (9)$$

and they assume that the quantum conditional min-entropy $H_{\min}(S|D)_\rho$ of the source conditioned on the device is greater than some constant k . This implies [3] that for any POVM measurement $\{\mathcal{M}_s\}$ performed by an agent on the quantum register D , the probability of the agent correctly guessing S , $P_{\text{guess}}(S|D)$ is upper bounded. From no-signaling, it follows that the distribution $P(S = s)$ is the same for every measurement input $I = i$ so that the joint distribution of variables is of the form $P(O = o, I = i, S = s) = P(O = o|I = i, S = s)P(I = i)P(S = s)$. The assumption of Chung, Shi and Wu thus implies that for any input variable I independent of the source S , the probability $P_{\text{guess}}(S|D)$ obeys

$$P_{\text{guess}}(S|D) = \sum_s P(O = s|I = i)P(S = s|O = s, I = i) \leq 2^{-k} \quad \forall i. \quad (10)$$

The above condition (whether in the scenario of a min-entropy source, or that of an SV source) has the drawback of effectively introducing an agent that is not correlated with the weak source. However we know that from two independent partially random sources one can extract perfect randomness in the classical world. So the operational realization of the originally mathematical condition might require the existence of an independent variable, implying the possibility of obtaining randomness right from the source and the agent's variable, if the latter's distribution was not deterministic.

In this paper, we consider a somewhat intermediate assumption: we assume that the agent (which we call the "tester") has a variable which describes subsequent bits drawn from the same SV source (so that his variable will not be necessarily independent of the other portion of the SV source, used as input by the users who want to draw randomness). However, we also assume that the device is correlated with the tester's variable only through the users' variable, i.e. that for any o, i, s, s' we have $P(O = o|I = i, S = s, S' = s') = P(O = o|I = i, S = s)$. This is a clearly weaker assumption than the SV-analogue of the CSW condition, since if we take S' to be independent of S , we obtain the CSW condition, while in our case this condition need not be met, and the dependence between S' and S may be chosen by an adversary. In other words, in the SV analogue of the CSW assumption, one requires that for some particular joint distribution (with independent I and S), $P(S|I, O)$ is still an SV source, irrespective of the protocol, while in our case, the latter may hold for some other distribution, this time chosen *adversarially* for any given protocol.

The threshold for the range of ε for which we will be able to amplify the SV source in the present paper (obtained in Theorems 11 and 18) is weaker than the one obtained by Colbeck

and Renner in [4]. This however is only to be expected as the scenario considered in this paper is more general than the scenario analyzed in [4], which was based on the assumption that the source and the device are independent. While the protocols of [5], [7] and [9] achieve randomness amplification for the entire range of ε and the latter two protocols also tolerate noise within a finite-device framework, they also do so under the assumption of independence between source and device and are therefore incomparable with the results in this paper.

D. Scenario

The scenario is as follows. There are: an ε -SV source and a device correlated to some portion of subsequent bits from the source, described by the variable S (see Fig. 4). The honest parties draw $S = s$ from the source and use it as an input to the box, which means that S and I_{HP} , the random variable describing the measurement settings of the honest parties, are perfectly correlated, i.e.

$$P(I_{HP} = i | S = s) = \delta_{is} \quad \text{for every } i, s. \quad (11)$$

The honest parties then test the statistics of a box for suitable violation of a certain Bell inequality.

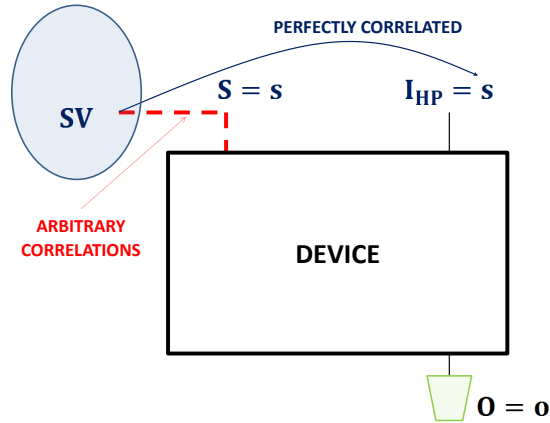


FIG. 4: Bits from an ε -SV source are used by honest parties as inputs. The correlation is given by Eq. (11).

E. The true and observed Bell value

In the most general form, the Bell value is given by the formula

$$\delta = \sum_{o,i} P(O = o, I = i) B(i, o), \quad (12)$$

where B is an indicator vector for the Bell inequality and P is an arbitrary joint probability distribution. We specify it depending on the context.

We are particularly interested in evaluating the true Bell value, as it informs us whether the box delivers randomness or not. Let \mathcal{I} denote all the settings appearing in the Bell expression. The

true Bell value δ^{true} is calculated for variables I_{indep} , uniformly distributed ($P(I_{\text{indep}} = i) = 1/|\mathcal{I}|$) and independent from S . It is then defined as follows

$$\delta^{\text{true}} = \frac{1}{|\mathcal{I}|} \sum_{o,i} P(O = o | I_{\text{indep}} = i) B(i, o), \quad (13)$$

where $|\mathcal{I}|$ is the number of measurement settings.

Further, we define the observed Bell value, i.e. we write Eq. (12) for I_{HP} , determined by Eq. (11), and obtain

$$\delta_{HP}^{\text{obs}} = \sum_{o,s} P(S = s) P(O = o | I_{HP} = s, S = s) B(s, o). \quad (14)$$

The aim is to show that the true Bell value is small whenever the observed value is small, i.e. the ratio $\delta_{HP}^{\text{obs}}/\delta_{SV}^{\text{true}}$ is controlled.

F. Testing the SV-condition for boxes

Honest parties test the statistics of a box using a certain Bell inequality. There is a danger that they may be cheated, as exemplified in Section II. The ε -SV source can be correlated with the device, as illustrated in Fig. 5 (on the left).

Since the honest parties only input I_{HP} which is perfectly correlated to S ,

$$P(I_{HP} = i | S = s) = \delta_{i,s}, \quad (15)$$

they are themselves not able to verify whether the SV-condition for boxes (7) is violated or not. Therefore, we consider testers who have access to part of the ε -SV source (SV_{test}), described by the variable S_{test} , which is correlated with the device only through the variable S and does not change the statistics of a box $P(O|I, S)$ (see Fig. 5, on the right), i.e.

$$p_{\min} \leq P(S_{\text{test}} = s' | S = s) \leq p_{\max} \quad \text{for every } s, s' \quad (16)$$

and

$$P(O|I, S, S_{\text{test}}) = P(O|I, S). \quad (17)$$

When honest parties take the portion of bits S from the main part of source (they do not have access to SV_{test}), to which the device is possibly correlated, the testers may be asked to perform the measurement using their bits S_{test} as input, i.e.

$$P(I_{\text{test}} = i' | S_{\text{test}} = s') = \delta_{i',s'}. \quad (18)$$

The overall picture is now the following. We have two different joint distributions $P(O, I, S, S_{\text{test}})$ and $P(O, I_{\text{test}}, S, S_{\text{test}})$. Conditional distributions are correlated as follows:

$$P(O = o | I = i, S = s, S_{\text{test}} = s') \stackrel{\text{Eq.(17)}}{=} P(O = o | I = i, S = s) \quad (19)$$

$$\stackrel{\text{Remark 1}}{=} P(O = o | I_{\text{test}} = i, S = s) \quad (20)$$

$$\stackrel{\text{Eq.(17)}}{=} P(O = o | I_{\text{test}} = i, S = s, S_{\text{test}} = s') \quad (21)$$

for every o, i, i', s, s' , where the pairs of variables I, S and $I_{\text{test}}, S_{\text{test}}$ are each perfectly correlated. As shown in Appendix I, we have that Eq. (16) implies

$$\zeta_{\min} \leq P(S = s | I_{\text{test}} = s') \leq \zeta_{\max}, \quad (22)$$

where ζ_{\min} and ζ_{\max} are functions of p_{\min}, p_{\max} and $|\mathcal{I}|$, explicitly given by Eq. (89) in Appendix I. Due to the SV-condition for boxes (7) this gives that

$$\zeta_{\min} \leq P(S = s | I_{\text{test}} = s', O = o) \leq \zeta_{\max} \quad \text{for every } s, s', o. \quad (23)$$

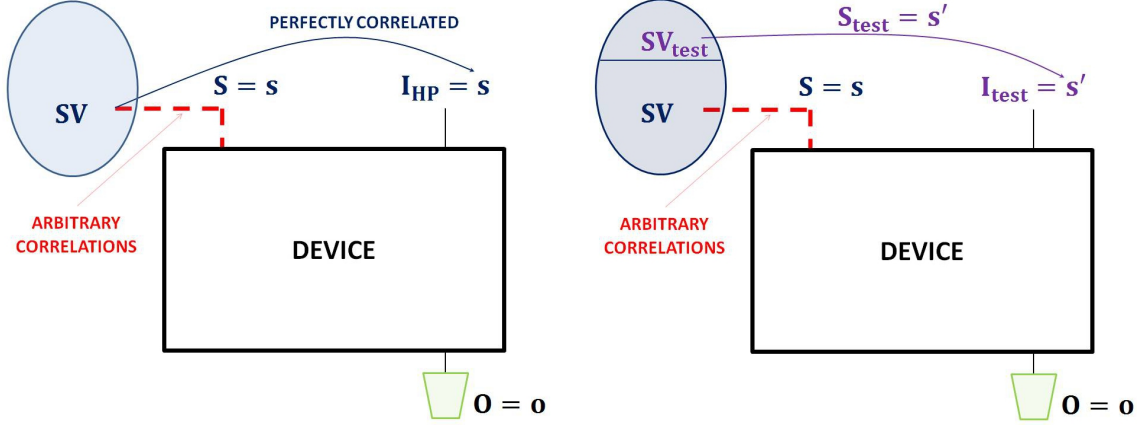


FIG. 5: (Left) The main part of the ε -SV source represented by variable S is correlated to the device, so that S determines the box. (Right) Other bits denoted by variable S_{test} from the part of the ε -SV source SV_{test} are correlated with the device only through the variable S . If bits are taken from SV_{test} and used as inputs to the device, one can check whether the SV-condition for boxes in Eq.(7) is violated.

We now introduce an intermediate value between δ_{HP}^{obs} and δ^{true} :

$$\delta_{SV}^{\text{true}} = \sum_{o, s'} P(O = o, I_{\text{test}} = s') B(s', o), \quad (24)$$

where I_{test} is a random variable satisfying Eq. (16). Note that, according to the observation in Remark 1, we obtain

$$\begin{aligned} \delta^{\text{true}} &\stackrel{\text{Eq. (13)}}{=} \frac{1}{|\mathcal{I}|} \sum_{o, i, s} P(S = s) P(O = o | I_{\text{indep}} = i, S = s) B(i, o) \\ &\stackrel{\text{Remark 1}}{=} \frac{1}{|\mathcal{I}|} \sum_{o, i, s} P(S = s) \frac{P(O = o, I_{\text{test}} = i, S = s) B(i, o)}{P(I_{\text{test}} = i, S = s)} \\ &= \frac{1}{|\mathcal{I}|} \sum_{o, i, s} \frac{1}{P(I_{\text{test}} = i | S = s)} P(O = o, I_{\text{test}} = i, S = s) B(i, o) \end{aligned} \quad (25)$$

and hence, according to Eq. (16) and the definition of $\delta_{SV}^{\text{true}}$ in Eq.(24), we have

$$\frac{1}{p_{\max} |\mathcal{I}|} \delta_{SV}^{\text{true}} \leq \delta^{\text{true}} \leq \frac{1}{p_{\min} |\mathcal{I}|} \delta_{SV}^{\text{true}}. \quad (26)$$

G. Results and proofs

At this point, let us explicitly restate all the assumptions used in the paper for clarity:

1. There are spatially separated honest parties who share a no-signaling box, i.e., one constrained by conditions Eq.(2).
2. Correlations between the source and the device are only limited by the SV-condition for boxes (see Eq. (7)). The device is correlated to the main part of the source from which honest parties draw their bits represented by variable S (see Eq. (11)).
3. There exists another part of the source, called SV_{test} , which may only be used (by testers) to verify whether the SV-condition for boxes is violated. S_{test} drawn from SV_{test} is only correlated with the device through the variable S and does not change the statistics of the box as given in Eq.(17).

The main result of this Section is the following.

Theorem 3. *Under assumptions 1-3 we obtain*

$$\frac{\delta_{HP}^{\text{obs}}}{\delta^{\text{true}}} \geq |\mathcal{I}| \frac{p_{\min} \zeta_{\min}}{p_{\max}}. \quad (27)$$

Proof. Note that Eqs. (23) and (16), as well as Remark 1, imply that

$$\begin{aligned} \delta_{HP}^{\text{obs}} &\stackrel{\text{Eq. (14)}}{=} \sum_{o,s} P(S=s) P(O=o | I_{HP}=s, S=s) B(s,o) \\ &\stackrel{\text{Remark 1}}{=} \sum_{o,s} P(S=s) P(O=o | I_{\text{test}}=s, S=s) B(s,o) \\ &= \sum_{o,s} P(S=s) \frac{P(O=o, S=s | I_{\text{test}}=s)}{P(S=s | I_{\text{test}}=s)} B(s,o) \\ &= \sum_{o,s} \frac{P(S=s) P(I_{\text{test}}=s)}{P(S=s, I_{\text{test}}=s)} P(S=s | O=o, I_{\text{test}}=s) P(O=o | I_{\text{test}}=s) B(s,o) \\ &\stackrel{\text{Eq. (23)}}{\geq} \zeta_{\min} \sum_{o,s} \frac{1}{P(I_{\text{test}}=s | S=s)} P(O=o, I_{\text{test}}=s) B(s,o) \\ &\stackrel{\text{Eq. (16), Eq. (18)}}{\geq} \frac{\zeta_{\min}}{p_{\max}} \sum_{s,o} P(O=o, I_{\text{test}}=s) B(s,o) \stackrel{\text{Eq. (24)}}{=} \frac{\zeta_{\min}}{p_{\max}} \delta_{SV}^{\text{true}}. \end{aligned} \quad (28)$$

Referring to Eq. (26), we obtain

$$\delta_{HP}^{\text{obs}} \geq |\mathcal{I}| \frac{p_{\min} \zeta_{\min}}{p_{\max}} \delta^{\text{true}}, \quad (29)$$

which completes the proof. \square

Remark 4. *Suppose that assumptions 1-3 are satisfied. Note that any Bell value (of non-local boxes) observed in a lab can be predicted by the rules of quantum mechanics and hence we set*

$$\delta_{HP}^{\text{obs}} = \delta_Q. \quad (30)$$

Further, due to Theorem 3, we obtain

$$\delta^{\text{true}} \leq \delta_Q \frac{p_{\max}}{|\mathcal{I}| p_{\min} \zeta_{\min}}, \quad (31)$$

where ζ_{\min} , p_{\min} and p_{\max} depend on both $|\mathcal{I}|$ and ε . The above inequality allows to set an upper bound for ε (as $|\mathcal{I}| \rightarrow \infty$), as illustrated in the example of the chained Bell inequality below.

IV. EXAMPLE - RANDOMNESS AMPLIFICATION USING CHAINED BELL INEQUALITIES

A. The chained Bell inequality

The chained Bell inequality considers the bipartite scenario of two spatially separated parties Alice and Bob. Let $n \in \mathbb{Z}_+$ be an arbitrary positive even integer. Let the sets $U_A := \{1, 3, \dots, n-1\}$ and $U_B := \{2, 4, \dots, n\}$ correspond to the measurement settings chosen by Alice and Bob, respectively. Each measurement pair (u, v) , where $u \in U_A$, $v \in U_B$, results in a binary outcome $x \in \{0, 1\}$ for Alice and $y \in \{0, 1\}$ for Bob. The chained Bell inequality is then written as [2]

$$\frac{1}{n} \left(\sum_{u,v:|u-v|=1} P(O = (x, y) | I = (u, v)) [x \oplus y = 1] + P(O = (x, y) | I = (1, n)) [x \oplus y = 0] \right) \geq \frac{1}{n}, \quad (32)$$

where \oplus denotes addition modulo 2 and $[B]$ denotes the Iverson bracket taking value 1 when B is true and 0 otherwise.

Remark 5. Note that out of the $n^2/4$ possible measurement pairs, only n neighbouring pairs, forming a chain, are considered in the inequality.

For clarity, we further label the inputs pairs by the number of the edge in the chain (see Remark 5), i.e., instead of a pair (u, v) , where $u \in U_A$, $v \in U_B$ and $|u - v| = 1$, we set $i := \min\{u, v\}$. Similarly, the remaining pair in a chain $(1, n)$ is denoted by n . Note that the true Bell value for an arbitrary box P is then given by

$$\delta^{\text{true}}(P) = \frac{1}{n} \left(\sum_{i \neq n} P(O = (x, y) | I = i) [x \oplus y = 1] + P(O = (x, y) | I = n) [x \oplus y = 0] \right), \quad (33)$$

while the observed value is of the form

$$\delta_{AB}^{\text{obs}}(P) = \sum_{s \neq n} P(S = s) P(O = (x, y) | I = s, S = s) [x \oplus y = 1] \quad (34)$$

$$+ P(S = n) P(O = (x, y) | I = n, S = n) [x \oplus y = 0]. \quad (35)$$

We recall that results observed in a lab are not better than the values predicted by the rules of quantum mechanics. Quantum mechanics violates (32) and provides a value of

$$\delta_Q := \sin^2(\pi/2n), \quad (36)$$

which tends to 0, as $n \rightarrow \infty$, with a rate of convergence $1/n^2$. This optimal quantum value is obtained by measuring on the maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with the measurement settings defined by the bases $\{|\alpha\rangle, |\alpha + \pi\rangle\}$, $\alpha \in \frac{\pi}{n}\{0, 2, \dots, n-2\}$, for Alice and $\{|\beta\rangle, |\beta + \pi\rangle\}$, $\beta \in \frac{\pi}{n}\{1, 3, \dots, n-1\}$, for Bob, where $|\cdot\rangle = \cos(\cdot/2)|0\rangle + \sin(\cdot/2)|1\rangle$.

B. Value of chained Bell inequalities on boxes

While testing the chained Bell inequality, we do not distinguish between boxes with the same probability distributions for neighboring pairs of settings. Hence, we consider only two types of extremal boxes: ideal or "bad". Any other box may be represented as a mixture of these boxes, due to the characterization of the extremal boxes for this scenario in [14].

We call boxes ideal (P_{ideal}) if they violate the chained Bell inequality (32) maximally and give perfectly random bits (boxes P_{ideal} play for the chained Bell inequality the same role as PR-boxes play for the CHSH inequality). With respect to the probability distributions significant for the chained Bell expression, there is exactly one box violating (32) to 0 (compare with Remark 5). Precisely, this is the no-signaling box with structure of perfect correlations for the $n-1$ neighboring pairs in the sum and a perfect anti-correlation for the remaining pair n (see [14] for details). Then,

$$\delta^{\text{true}}(P_{\text{ideal}}) = \frac{1}{n} \left(\sum_{i \neq n} P_{\text{ideal}}(O = (x, y) | I = i) [x \oplus y = 1] + P_{\text{ideal}}(O = (x, y) | I = n) [x \oplus y = 0] \right) = 0. \quad (37)$$

In classical theory, there are no ideal boxes. The notion P_{bad} is used for these extremal (local deterministic) boxes whose Bell value is at least $1/n$, which means that there is at least one contradiction with probability distributions of ideal boxes (for neighboring pairs of settings). Apart from purely classical boxes there are also other bad boxes which do not violate the chained Bell inequality (32) (some of them even give randomness, but are inappropriate for the chosen inequality (32)). Convex combinations of boxes P_{bad} are denoted by P_{BAD} . By convexity,

$$\delta^{\text{true}}(P_{\text{BAD}}) \geq 1/n. \quad (38)$$

Remark 6. Any box P is a mixture of boxes which attain an optimal Bell value 0 and boxes which do not violate the chained Bell inequality

$$P = (1 - \Lambda_P) P_{\text{ideal}} + \Lambda_P P_{\text{BAD}}, \quad \Lambda_P \in [0, 1]. \quad (39)$$

Corollary 7. The true Bell value for an arbitrary box P is estimated as follows

$$\delta^{\text{true}}(P) \geq \Lambda_P/n, \quad (40)$$

where Λ_P is defined by Eq. (39).

Proof. Note that, according to Remark 6, we obtain

$$\delta^{\text{true}}(P) \stackrel{\text{Eq. (39)}}{=} \delta^{\text{true}}((1 - \Lambda_P) P_{\text{ideal}} + \Lambda_P P_{\text{BAD}}) = (1 - \Lambda_P) \delta^{\text{true}}(P_{\text{ideal}}) + \Lambda_P \delta^{\text{true}}(P_{\text{BAD}}) \quad (41)$$

$$\stackrel{\text{Eq. (37)}}{=} \Lambda_P \delta^{\text{true}}(P_{\text{BAD}}) \stackrel{\text{Eq. (38)}}{\geq} \Lambda_P/n. \quad (42)$$

□

C. The chained Bell inequality and randomness

Let $I = i$, for $i \in \{1, \dots, n\}$ be any chosen input to a box P . To measure the distance between an output bit and a random bit obtained from the box P we introduce the following quantity

$$d(P) = \max_i \{d_i(P)\}, \quad (43)$$

where

$$d_i(P) = \frac{1}{2} \left(\left| p_i^{(P)}(0) - 1/2 \right| + \left| p_i^{(P)}(1) - 1/2 \right| \right), \quad (44)$$

and

$$\begin{aligned} p_i^{(P)}(x) &= \sum_{y \in \{0,1\}} P(O = (x, y) | I = i) [x \oplus y = 0] \quad \text{for } i \in \{1, \dots, n-1\}, \\ p_n^{(P)}(x) &= \sum_{y \in \{0,1\}} P(O = (x, y) | I = n) [x \oplus y = 1] \end{aligned} \quad (45)$$

for $x \in \{0, 1\}$. Note that for boxes P_{ideal} , which generate randomness, we have $p_i^{P_{\text{ideal}}}(0) = p_i^{P_{\text{ideal}}}(1) = 1/2$ for every i . Due to Eq. (39), we further obtain

$$p_i^{(P)}(x) = \Lambda_P p_i^{\text{BAD}}(x) + (1 - \Lambda_P) \frac{1}{2}, \quad (46)$$

where p_i^{BAD} is generated by boxes P_{BAD} and, in the worst case, it is some deterministic function.

Proposition 8. *Let $d(P)$ be defined by Eq. (43) for every box P of the form (39). Then*

$$d(P) \leq \frac{\Lambda_P}{2} \leq \frac{n}{2} \delta^{\text{true}}(P). \quad (47)$$

Proof. Let us bound the distance d from above. Following Eqs. (43) and (46), we obtain

$$d(P) = \frac{\Lambda_P}{2} \max_i \{ |p_i^{\text{BAD}}(0) - 1/2| + |p_i^{\text{BAD}}(1) - 1/2| \} \leq \frac{\Lambda_P}{2}. \quad (48)$$

Note that, due to Eq. (40) of Corollary 7, we obtain that

$$d(P) \leq \frac{\Lambda_P}{2} \leq \frac{n}{2} \delta^{\text{true}}(P), \quad (49)$$

which completes the proof and indicates that small true chained Bell value of any box P guarantees that the distribution of the output bit obtained from it is close to uniform. \square

D. Randomness versus observed Bell value

Theorem 3 and Remark 4 imply for the chained Bell inequality that provided we observe a Bell value of δ_Q from a box P , i.e., $\delta_{HP}^{\text{obs}}(P) = \delta_Q$, then the true Bell value of the box can be bounded as

$$\delta^{\text{true}}(P) \leq \delta_Q \frac{p_{\max}}{np_{\min} \zeta_{\min}}, \quad (50)$$

where δ_Q is given by Eq. (36) and

$$p_{\min} := \frac{p_-^{2r}}{np_+^{2r}}, \quad p_{\max} := \frac{p_+^{2r}}{p_+^{2r} + (n-1)p_-^{2r}}, \quad \zeta_{\min} = \frac{p_{\min}^2}{np_{\max}^2} \quad (51)$$

for $r = \log(n/2)$. The estimates come from [4] and Appendix I and are obtained using Remark 5. Even more accurate estimates are given in [12]. Furthermore, we have that the distance of the output bit obtained from the box with such an observed value can be bounded as follows.

Proposition 9. For $d(P)$ given by Eq. (43) we obtain

$$d(P) \leq \delta_Q \frac{p_{\max}}{2p_{\min}\zeta_{\min}}. \quad (52)$$

Proof. The proof is an easy observation, which follows from Proposition 8 and Theorem 3, as well as Remark 4 (see Eqs. (47) and (50)). \square

Remark 10. In the next Subsection we determine the threshold for ε , below which the right hand side of inequality (52) tends to zero, as $n \rightarrow \infty$, and hence almost full randomness of output bits is obtained.

E. Calculating the threshold for ε

Let us restate the assumptions in the context of the chained Bell inequality:

1. Alice and Bob are spatially separated and share a no-signaling box with two input sets of size $n/2$ and two binary outputs, which violates the chained Bell inequality up to δ_Q . They choose their settings, each using $r = \log(n/2)$ bits from the main part of the ε -SV source (n is taken to be an appropriate integer of the form 2^{r+1}), i.e., the variable I_{HP} describing their inputs, is perfectly correlated with S as in Eq.(11).
2. The SV-condition for boxes (7) is satisfied with $p_{\min}, p_{\max}, \zeta_{\min}$ given by (51).
3. The main part of the source is correlated with the device used by Alice and Bob. Another part, called SV_{test} , is not directly correlated with a device, it is only used to check whether the SV-condition for boxes is violated (details are described in Section III.E).

Theorem 11. Assume that conditions 1-3 are satisfied. Then, $\varepsilon < \frac{(2^{1/12}-1)}{2(2^{1/12}+1)}$ (≈ 0.0144) guarantees full randomness of the output in the asymptotic scenario of a large number of inputs $n \rightarrow \infty$.

Remark 12. The threshold is in fact slightly bigger (precisely it is $\frac{(2^{1/6(2-c)}-1)}{2(2^{1/6(2-c)}+1)} \approx 0.0162$ where c solves $H(c/2) = 1/2$ for the binary entropy H), which can be proven with more accurate approximations for p_{\min}, p_{\max} and ζ_{\min} , obtained by using the Ky Fan norm (see [12]), i.e., in the regime of large n

$$p_{\min} = \frac{p_-^{2r}}{p_-^{2r} + 2^r p_+^{(2-c)r} p_-^{cr}} \quad p_{\max} = \frac{p_+^{2r}}{p_+^{2r} + 2^r p_-^{(2-c)r} p_+^{cr}}. \quad (53)$$

Proof. Proposition 9 and Remark 10 imply that to verify that output bits are fully random ($d \rightarrow 0$) it is enough to show that

$$\Delta := \delta_Q \frac{p_{\max}}{2p_{\min}\zeta_{\min}} \rightarrow 0, \quad \text{as } n \rightarrow \infty. \quad (54)$$

Following Eqs. (36), (51), we obtain

$$\begin{aligned} \Delta &= \frac{1}{2} \sin^2\left(\frac{\pi}{2n}\right) \frac{p_{\max}}{p_{\min} \frac{p_{\min}^2}{np_{\max}}} \leq \frac{1}{2} \left(\frac{\pi}{2n}\right)^2 \frac{np_{\max}^3}{p_{\min}^3} = \left(\frac{\pi^2}{8}\right) \frac{1}{n} \frac{p_{\max}^3}{p_{\min}^3} \\ &= \left(\frac{\pi^2}{8}\right) \frac{1}{n} \frac{p_+^{6r}}{(p_+^{2r} + (n-1)p_-^{2r})^3} \frac{n^3 p_+^{6r}}{p_-^{6r}} \\ &= \left(\frac{\pi^2}{8}\right) \frac{n^2 p_+^{12r}}{p_-^{6r} (p_+^{2r} + (n-1)p_-^{2r})^3} \end{aligned} \quad (55)$$

Setting $n = 2^{r+1}$, we have

$$\Delta = \left(\frac{\pi^2}{8}\right) \frac{4^{r+1} p_+^{12r}}{p_-^{6r} (p_+^{2r} + (2^{r+1} - 1) p_-^{2r})^3}. \quad (56)$$

Let us now consider the asymptotic scenario of a large number of settings $r \rightarrow \infty$,

$$\lim_{r \rightarrow \infty} \frac{4^{r+1} p_+^{12r}}{p_-^{6r} (p_+^{2r} + (2^{r+1} - 1) p_-^{2r})^3} = 0, \quad (57)$$

which imposes that ε is bounded as

$$\varepsilon < \frac{2^{1/12} - 1}{2(2^{1/12} + 1)} \approx 0.0144. \quad (58)$$

Therefore, for the range $0 \leq \varepsilon < \frac{2^{1/12}-1}{2(2^{1/12}+1)}$, we obtain a random output in the asymptotic scenario of a large number of inputs. \square

V. THE PROTOCOL FOR THE CHAINED BELL INEQUALITY

Protocol
<ol style="list-style-type: none"> 1. The honest parties Alice and Bob choose their measurement settings $u_i \in U_A, v_i \in U_B$ for each of the runs $i = 1, \dots, M$ where the input sets are of size $U_A = U_B = n/2$ (see Section IV A for the precise definitions of U_A, U_B). To do so, in each run they use $\log_2(n/2)$ bits from an ε-SV source. Simultaneously, a sequence of M boxes is supplied. 2. They check that the cardinality \mathcal{S} of the set \mathcal{S} defined as $\mathcal{S} := \{i \in \{1, \dots, M\} : u_i - v_i = 1 \vee (u_i, v_i) = (1, n)\} \quad (59)$ satisfies $\mathcal{S} \in [\frac{2M}{n}, \frac{6M}{n}]$. If not, they set the output to $R = \text{Fail}$ and abort the protocol. 3. They verify that $x_i = y_i$ for every $i \in \mathcal{S}, (u_i, v_i) \neq (1, n)$ or $x_i \neq y_i$ for $i \in \mathcal{S}, (u_i, v_i) = (1, n)$. If any one of these conditions is not satisfied, they set $R = \text{Fail}$ and abort. 4. They use further bits from the ε-SV source to choose $f \in \mathcal{S}$ which indicates the position of the box, from which an output bit x_f is recorded. The protocol outputs $R = x_f$.

Remark 13. In Step 1, we require $|\mathcal{S}| \in [2M/n, 6M/n]$, since the probability of uniformly choosing neighboring measurement settings is exactly $P(i \in \mathcal{S}) = 4/n$, for every $i \in \{1, \dots, M\}$.

Remark 14. In the proof we set $M := (n/2)^{2.99}$ and take n such that $\log n$ and $\log M/n$ are integers. We have that $(2M)/n = (n/2)^{1.99}$ and $(6M)/n = 3(n/2)^{1.99}$ and the number of boxes labeled by $i \in \mathcal{S}$ is slightly smaller than $(n/2)^2$ (for large n). This ensures that the protocol does not abort when run with the optimal quantum strategy while it does abort when run with classical boxes.

VI. ANALYSIS OF THE RANDOMNESS AMPLIFICATION PROTOCOL

A. Parameters

The parameters of the general problem are denoted by m , n and a . Here m is the number of boxes (runs) in the protocol ($m = |\mathcal{S}|$ in the protocol above based on the chained Bell inequality), n is the number of input pairs that enter the inequality and a is the probability that in any run, a local box attempting to mimic an ideal box is *not* detected by the measurement.

B. Attacks on the protocol due to lack of independence

Consider that an adversary prepares a sequence of boxes of length m , and the honest parties obtain bits from the source to input as measurement settings in the runs $i = 1, \dots, m$. In the previously considered scenario in [4], the assumption of independence between the source and device implies that the observation by the honest parties of the ideal sequence of measurement outcomes (i.e., compatible with the optimal violation) guarantees that the true Bell value of the devices used in the protocol is also optimal. Moreover, the distribution of the further bits drawn to choose $f \in \mathcal{S}$ (the position of the box from which the final output bit is drawn) is also independent of the device. Therefore, when the tests in the protocol are passed, the boxes used must be optimal (i.e., as $n \rightarrow \infty$, we have that $\delta^{true} \rightarrow 0$ faster than $\frac{1}{n}$), and perfect randomness may be obtained from the output.

The relaxation of the independence assumption means that the sequence of boxes supplied by the adversary may be correlated with the bits that the honest parties use in the protocol. This implies that for any given sequence of inputs and corresponding observed outputs ($I = i, O = o$), there is a class of box sequences that is compatible with this (i, o) . We denote such a class in what follows as a "cloud" of box sequences. Moreover, the bit string corresponding to position f is drawn from the same SV source, which means that the SV-condition for boxes in Eq.(7) applies to it. We will therefore consider attacks limited by the SV-condition as in the following remarks.

Remark 15. Correlations between measurement settings from the source and boxes are the same as in Sections III and IV, so only the SV-condition for boxes (7) limits them.

Remark 16. We allow attacks in which correlations between sequences of $|\mathcal{S}|$ boxes and the number f are only limited as in Eq.(68) which follows from the SV- condition for boxes.

However, we do not solve the case of the most general attack strategy limited by these two remarks in this paper, and will also make some further "symmetry" assumptions on the attack strategies that we will make explicit in what follows.

C. Types of sequences

See Section IV to recall what is meant by ideal and bad boxes. Let us introduce the following notation. We say that a sequence of extremal boxes is of type j if it contains exactly j bad boxes.

Let P_j denote the probability of the class of box sequences of type j . Obviously,

$$\sum_{j=1}^m P_j = 1. \quad (60)$$

Note that within a sequence of m boxes, j bad boxes may be arranged in $\binom{m}{j}$ different ways (see Fig. 6)

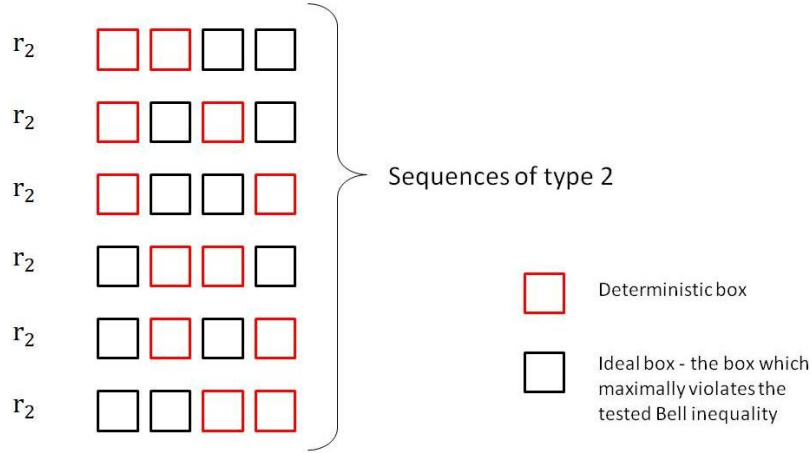


FIG. 6: Possible arrangements of two bad boxes in a sequence of four boxes.

Let us consider the case when any bad box has exactly one contradiction when compared with the correlations in an ideal box. In this case, there are $\binom{m}{j} n^j$ possible sequences of type j (since the contradiction can happen in any one of the n different measurement pairs, see an example in Fig. 7). Furthermore, consider the case when every sequence of type j is equally likely, i.e. appears with the same probability r_j , this gives that

$$P_j = \binom{m}{j} n^j r_j. \quad (61)$$

D. The notion of clouds

If we measure a bad box, we may either observe a contradiction with the correlations in an ideal box or not. Not observing a contradiction does not guarantee that the box is ideal. This leads to the notion of clouds, i.e., classes of boxes compatible with a given sequence of observations for a chosen sequence of measurement inputs. If 1 denotes the event that a contradiction is observed and 0 denotes the complementary event, the pattern of zeros and ones (of length m), together with the chosen sequence of measurement settings, defines the cloud. Let a sequence of measurement settings be fixed. We denote the cloud by $\mathcal{C}^{\mathbf{l}}$, where $\mathbf{l} = (l_1, \dots, l_m)$ and $l_1, \dots, l_m \in \{0, 1\}$. Note that $|\mathbf{l}| = \sum_{j=1}^m l_j$ delivers information about the number of detected contradictions, hence detected bad boxes. So there are at least $|\mathbf{l}|$ bad boxes in the sequence which has been measured (see Figs. 8 and 9). Hence, in every cloud $\mathcal{C}^{\mathbf{l}}$ there are boxes of type q for $q \geq |\mathbf{l}|$, but only of certain arrangements, determined by the performed measurements (see Fig. 8 for an example set of arrangements).

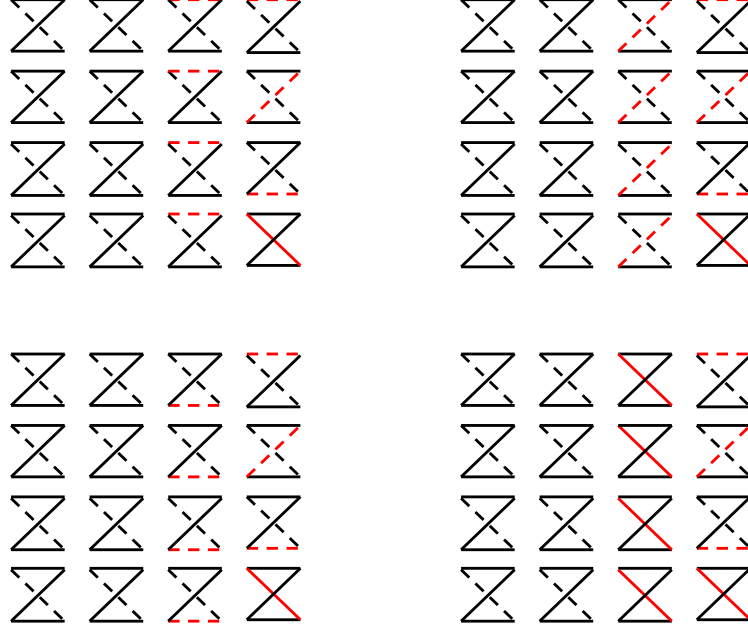


FIG. 7: There are n^j sequences of type j and of certain arrangement, e.g. in case of CHSH inequality, 16 different sequences are of type 2 and arrangement: 2 PR-boxes and 2 bad boxes. The edges with mismatched correlations are marked in red.

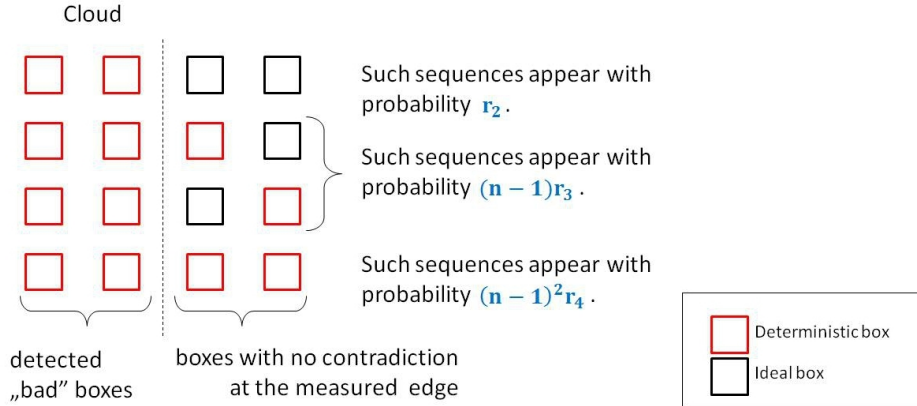


FIG. 8: The cloud $\mathcal{C}^{(1,1,0,0)}$ (with 2 detected bad boxes). First two boxes are bad, which is known after performing a measurement, the next two may be either ideal or bad boxes.

Note that detecting a contradiction gives certainty that the box is bad, as well as the knowledge where exactly the contradiction appears. Not detecting a contradiction delivers only information that there is no contradiction at the certain edge which has been measured. We may not exclude the possibility that there is a contradiction at any other (non-measured) edge (which is also indicated in the example in Fig. 8). It should be noted that clouds overlap at each other, i.e., the same sequence of boxes may appear in multiple clouds. Let $Q_l = P(\mathcal{C}^l)$ for $|l| = l$. Referring to the

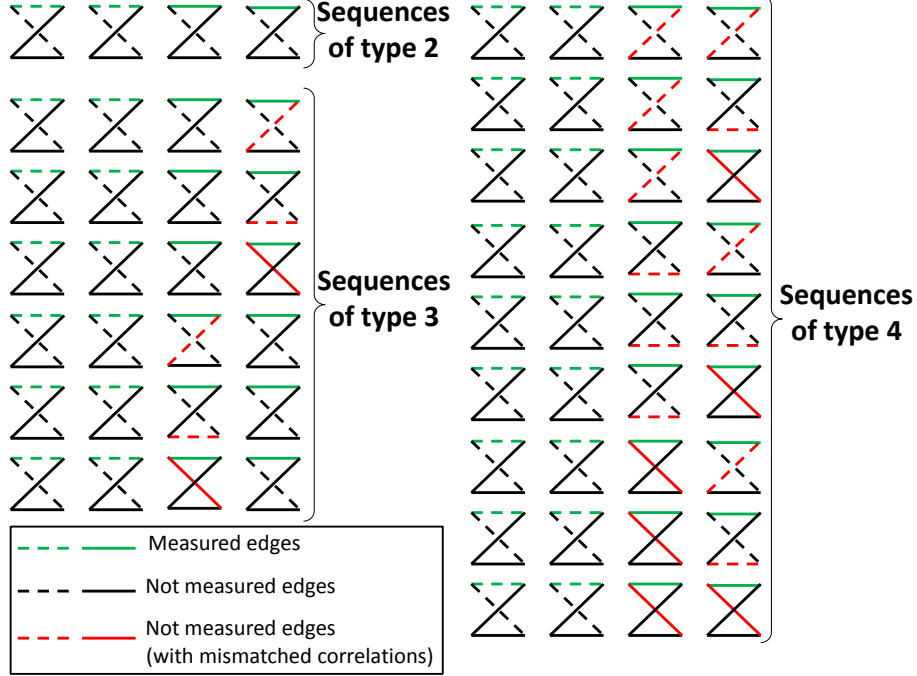


FIG. 9: The cloud $\mathcal{C}^{(1,1,0,0)}$ in case of CHSH inequality. First two boxes are bad, which is known after performing a measurement, the next two may be either PR-boxes or bad boxes.

above analysis, we obtain

$$Q_l = \sum_{s=0}^{m-l} \binom{m-l}{s} (n-1)^s r_{l+s} \quad \text{for } l \in \{1, \dots, m\}. \quad (62)$$

Note that there are $\binom{m}{l}$ clouds which appear with probability Q_l .

E. The attack strategy

Let us consider an attack strategy of the adversary that attempts to pass the protocol with a classical box of true Bell value at least $1/n$ so that honest parties are not able to obtain a random bit.

Recall that $f \in \{1, \dots, m\}$ is the number drawn using bits from the ε -SV source, which indicates the position of a box in a sequence from which the final bit is recorded. Let an arbitrary sequence of type k be denoted by Seq_k . Then, we consider the attack strategy given by the joint probability of f and all possibly supplied sequences which satisfy the following condition

$$P(f = i | \text{Seq}_k) = \begin{cases} 1/k & \text{for } i \in \{\text{indices defining the position of bad boxes in Seq}_k\} \\ 0 & \text{for } i \in \{\text{indices defining the position of ideal boxes in Seq}_k\}. \end{cases} \quad (63)$$

The attack is exemplified in Fig. 10.

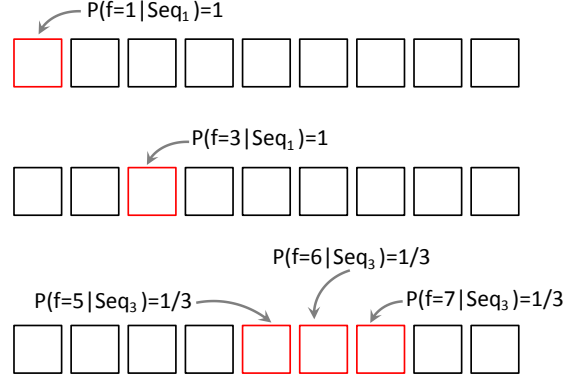


FIG. 10: The probability of f is spread uniformly over bad boxes.

F. Assumptions on the attack strategy

We assume that in the attack strategy, any bad box has exactly one contradiction when compared with the correlations in an ideal box. That any attack strategy without this assumption is strictly weaker is justified in Appendix II, intuitively it is clear that using local boxes with more contradictions simply decreases the probability of acceptance for the protocol (since the observed Bell value increases) in comparison to using boxes with a single contradiction while yielding the same lack of randomness in the output.

After taking the above considerations into account, we end with the following assumptions on the particular attack considered in this paper, whose relaxation might lead to a stronger attack on the protocol considered, and will therefore be investigated in future work.

1. We assume that the attack is symmetric in the sense that every box sequence of a particular type j (i.e., consisting of j bad boxes) appears with the same probability as in Eq.(61).
2. We assume that in the attack, the f drawn from the source is distributed uniformly over the bad boxes for any particular sequence Seq_k as specified in Eq. (63).
3. We assume that the attack consists of box sequences made of extremal boxes for each run, and defer the consideration of the general attack consisting of a large box coherent over all runs for future work.

To be consistent with assumption 2, we also set the probability that the adversary supplies the box sequence consisting of only ideal boxes to be zero, i.e., $P_0 = 0$, these boxes generate perfect random output over all runs so that using such boxes does not give any advantage to the adversary.

G. Probability of acceptance of the protocol

Recall that a denotes the probability of not detecting a contradiction with the correlations of an ideal box when measuring a bad box in a single run. Then, the probability of not aborting the

protocol, which happens if and only if the correlations in all the runs are compatible with the ideal correlations, is described by the following expression

$$P(\text{ACC}) = \sum_{k=1}^m P_k a^k. \quad (64)$$

In this scenario, the protocol does not abort, the attack succeeds and the honest parties do not obtain randomness. Let us now compute a for the protocol based on the chained inequality. Note that, since only one measurement can be performed, the probability that an edge with contradiction is measured is, in case of uniform and independent inputs, as small as $1/n$ and is even smaller in the case of inputs taken from the source. Due to Theorem 3,

$$n\delta^{\text{true}} \left(\frac{p_{\min}\zeta_{\min}}{p_{\max}} \right) \leq \delta^{\text{obs}}, \quad (65)$$

so that the probability that an edge with contradiction is measured by Alice and Bob is bounded from below by $p_{\min}\zeta_{\min}/p_{\max}$, which in turn implies that

$$a = 1 - \frac{p_{\min}\zeta_{\min}}{p_{\max}}. \quad (66)$$

Note that when we consider the probability of not detecting that a subsequent box is local, it is a conditional probability with all proceeding measurements in the condition (see Remark 2 in Section III about an arbitrary random variable e that is prior to the protocol).

In the rest of the paper, we will show that the protocol stays secure under the attack described, i.e., it aborts if the attack described by Eq. (63), is performed.

H. Constraints following from the SV-condition for boxes

We have that $p_-^{\log m} \leq P(f = i | \text{a sequence of measurements}) \leq p_+^{\log m}$, since f is a bit string drawn from the ε -SV source after the bits corresponding to the sequence of measurements are drawn from the same source. The assumed SV-condition for boxes in Eq.(7) then implies that

$$p_-^{\log m} \leq P(f = i | \text{a sequence of measurements and outcomes}) \leq p_+^{\log m} \quad (67)$$

for every $i \in \{1, \dots, m\}$. Note that there is a one-to-one correspondence between the sequence of measurements and outcomes and its corresponding cloud. Suppose that measurement settings are fixed and some outcomes are obtained. Then the appropriate cloud \mathcal{C}^1 is determined and we have

$$p_-^{\log m} \leq P(f = i | \mathcal{C}^1) \leq p_+^{\log m} \quad \text{for } i \in \{1, \dots, m\}. \quad (68)$$

Let us set $c_+ := p_+^{\log m}$ and $k := |\mathbf{l}|$. Since $P(\text{ACC})$, given by Eq. (64), is defined in terms of probabilities P_k (see Eq. (61)), condition (68) should also be rewritten in this way. Due to the definition of attack (see Eq. (63)) and the properties of clouds, we obtain

$$\sum_{s=0}^{m-k} \left(\frac{1}{k+s} - c_+ \right) \binom{k+s}{k} \left(\frac{n-1}{n} \right)^s P_{k+s} \leq 0. \quad (69)$$

The derivation of Eq.(69) is given in Appendix III.

I. Probability of acceptance as a linear program

The probability of acceptance can therefore be formulated as the following linear program. We want to maximize the expression

$$\sum_{k=1}^m P_k a^k \quad (70)$$

such that

$$\sum_{s=0}^{m-k} \left(\frac{1}{k+s} - c_+ \right) \binom{k+s}{k} \left(\frac{n-1}{n} \right)^s P_{k+s} \leq 0 \quad \text{for every } k \in \{1, \dots, m\}, \quad (71)$$

$$\sum_{k=1}^m P_k \leq 1 \quad \text{and} \quad \sum_{k=1}^m -P_k \leq -1, \quad (72)$$

where the problem constraints follow from Eqs. (69) and (61). Obviously,

$$P_k \geq 0 \quad \text{for every } k \in \{1, \dots, m\}. \quad (73)$$

Note that the linear program written above is at once in its standard form, that is

$$\begin{aligned} & \max \{ \vec{c}^T \vec{x} \} \\ & \text{such that } A\vec{x} \leq \vec{b} \\ & \text{and the variables are non-negative } \vec{x} \geq 0, \end{aligned} \quad (74)$$

where $\vec{x} = (P_1, \dots, P_m)^T$, $\vec{c} = (a, a^2, \dots, a^m)^T$, $\vec{b} = (0, \dots, 0, 1, -1)^T$ and A is a $(m+2) \times m$ matrix

$$A = \begin{bmatrix} \binom{1}{0} \left(\frac{n-1}{n} \right)^0 (1 - c_+) & \binom{2}{1} \left(\frac{n-1}{n} \right)^1 \left(\frac{1}{2} - c_+ \right) & \binom{3}{2} \left(\frac{n-1}{n} \right)^2 \left(\frac{1}{3} - c_+ \right) & \dots & \binom{m}{m-1} \left(\frac{n-1}{n} \right)^{m-1} \left(\frac{1}{m} - c_+ \right) \\ 0 & \binom{2}{0} \left(\frac{n-1}{n} \right)^0 \left(\frac{1}{2} - c_+ \right) & \binom{3}{1} \left(\frac{n-1}{n} \right)^1 \left(\frac{1}{3} - c_+ \right) & \dots & \binom{m}{m-2} \left(\frac{n-1}{n} \right)^{m-2} \left(\frac{1}{m} - c_+ \right) \\ 0 & 0 & \binom{3}{0} \left(\frac{n-1}{n} \right)^0 \left(\frac{1}{3} - c_+ \right) & \dots & \binom{m}{m-3} \left(\frac{n-1}{n} \right)^{m-3} \left(\frac{1}{m} - c_+ \right) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \binom{m}{0} \left(\frac{n-1}{n} \right)^0 \left(\frac{1}{m} - c_+ \right) \\ 1 & 1 & 1 & \dots & 1 \\ -1 & -1 & -1 & \dots & -1 \end{bmatrix}. \quad (75)$$

J. Dual problem

We consider the dual problem:

$$\begin{cases} \min \{ \vec{b}^T \vec{y} \} \\ A^T \vec{y} \geq \vec{c} \\ \vec{y} \geq 0. \end{cases} \quad (76)$$

By linear programming duality, if either the primal or dual has an optimal solution, then both have optimal solutions and the optimal values of the objective functions of these problems are equal.

In our case the dual problem is as follows

$$\min\{y_{m+1} - y_{m+2}\} \quad (77)$$

such that

$$\sum_{r=0}^{k-1} \binom{k}{r} \left(\frac{n-1}{n}\right)^r \left(\frac{1}{m} - c_+\right) y_{k-r} + y_{m+1} - y_{m+2} \geq a^k \quad \text{for } k \in \{1, \dots, m\} \quad (78)$$

and

$$y_1 \geq 0, \quad \dots, \quad y_m \geq 0, \quad y_{m+1} \geq 0, \quad y_{m+2} \geq 0. \quad (79)$$

We find the following feasible solution to the dual, formulated as Lemma 17 and proven in Appendix IV.

$$y_1 = \frac{a^{1/c_+}(1-a)}{\left(\frac{1}{c_+} + 1\right) \left(\frac{n-1}{n}\right)^{1/c_+}}, \quad y_2 = y_3 = \dots = y_m = y_{m+2} = 0, \quad y_{m+1} = a^{1/c_+}. \quad (80)$$

Lemma 17. *Hypothesis (80) gives a feasible solution of dual problem described by Eqs. (77) and (78).*

K. The optimal solution

In fact, Eq.(80) is not only a bound on the probability of acceptance but is in fact an optimal solution to the linear program. To prove that the above solution is optimal, we will show that the objective functions of both, primal and dual, problems are equal.

Suppose that the solution of the primal problem is given by

$$P_u = \frac{1}{(1 + s(u, v))}, \quad P_v = \frac{s(u, v)}{(1 + s(u, v))}, \quad P_k = 0 \quad \text{for } k \notin \{u, v\}, \quad (81)$$

where

$$s(u, v) = \frac{un(c_+ - 1/u)}{v(n-1)(1/v - c_+)} > 0 \quad \text{for } u \leq \frac{1}{c_+} \leq v. \quad (82)$$

If we set

$$u = \frac{1}{c_+}, \quad v = \frac{1}{c_+} + 1, \quad (83)$$

we obtain $P_{1/c_+} = 1$ and $P_{(1/c_++1)} = 0$ and therefore

$$\max \left\{ \sum_{k=1}^m P_k a^k \right\} = a^{1/c_+} = \min \{y_{m+1} - y_{m+2}\}, \quad (84)$$

which indicates that the solution is indeed optimal. However, we should note that to be more accurate, we should take u and v as natural numbers, i.e.

$$u = \left\lfloor \frac{1}{c_+} \right\rfloor, \quad v = \left\lfloor \frac{1}{c_+} \right\rfloor + 1. \quad (85)$$

L. Results for the chained Bell inequality

Set $a = (1 - p_{\min}\zeta_{\min}/p_{\max})$ (from Section VI.E) and $m = |\mathcal{S}| = (n/2)^{1.99}$ (which follows from the requirements of the protocol and the rules of quantum mechanics, see Remark 14). We approximate terms p_{\min} , p_{\max} and ζ_{\min} as we did in Eq. (51). Using the solution of linear programming from the previous section, we obtain that $P(\text{ACC})$ is bounded from above by

$$a^{1/(p_+^{\log_2(m)})}. \quad (86)$$

The bound converges to zero, as $n \rightarrow \infty$, for every ε solving the inequality

$$(0.5 - \varepsilon)^{12} - 2(0.5 + \varepsilon)^{13.99} > 0, \quad (87)$$

which approximately gives $0 < \varepsilon < 0.0132$.

The main result of this Section is hence the following.

Theorem 18. *Assuming the correlations between the source and device are constrained as in Remarks 15, 16 and under the assumptions on the attack strategy outlined in Section VI.F, the protocol in Section V is safe for $\varepsilon < 0.0132$ (or more precisely for ε solving the inequality $(0.5 - \varepsilon)^{12} - 2(0.5 + \varepsilon)^{13.99} > 0$).*

Remark 19. *The threshold is in fact slightly bigger than 0.0132, which can be proven with more accurate approximations for p_{\min} , p_{\max} and ζ_{\min} , obtained by using the Ky Fan norm (from [12].)*

M. Summary and closing remarks

We have studied the protocol of Colbeck and Renner [4] under relaxed assumptions which allow for correlations between the Santha-Vazirani source with the devices used in the protocol. We have proven, that in spite of such an attack, a non-zero range of parameter of ε -SV source allows for randomness amplification in the asymptotic limit of a large number of settings. More precisely, the protocol (see Section V) is safe for a restricted range of ε even if we admit

- (1) correlations between measurement settings and devices, only limited by the SV-condition for boxes (see Sections III and IV),
- (2) attacks such that f is always pointing to local boxes, i.e. boxes with no intrinsic randomness (correlations of sequences of boxes with f are only limited by condition (68), described in details in Section VI).

Our intuition, based on the experience gained while working with the SV-condition for boxes, is that the attacks, which we analyze in this paper are the strongest possible. Nevertheless, it is not yet formally proven that we can admit the symmetry assumptions in the attack without loss of generality. This is the aim for future work. Another interesting line of research, which is already in progress, aims to determine whether the attack can be physically performed or not, i.e., whether the correlations between the weak source and the devices can be created by the adversary physically without breaking the SV condition at this stage. Finally, an important open question is whether the techniques used in this paper can be generalized to relax the assumption of independence in the finite-device protocols of [7], [9] so as to obtain randomness amplification for the entire range of ε , while tolerating a constant level of noise.

Acknowledgments. We acknowledge useful discussions with Roger Colbeck, Renato Renner, Christopher Portmann, Gilles Pütz and Maciej Stankiewicz. This work is supported by the EU grant RAQUEL, and the ERC AdG QOLAPS.

-
- [1] R. Arnon-Friedman, A. Ta-Shma, *Limits of privacy amplification against non-signalling memory attacks*, Phys. Rev. A 86, 062333 (2012).
 - [2] S.L. Braunstein & C.M. Caves, *Wringing out better Bell inequalities*, Annals of Physics 202, 22 (1990).
 - [3] R. Koenig, R. Renner & C. Schaffner, *The operational meaning of min- and max-entropy*, IEEE Trans. Inf. Th., vol. 55, no. 9 (2009).
 - [4] R. Colbeck & R. Renner, *Free randomness can be amplified*, Nature Physics 8, 450-454 (2012).
 - [5] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, & A. Acin, *Full randomness from arbitrarily deterministic events*, Nature Communications 4, 2654 (2013).
 - [6] P. Mironowicz, R. Gallego & M. Pawłowski, *Amplification of arbitrarily weak randomness*, Phys. Rev. A 91, 032317 (2015).
 - [7] F.G.S.L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek & H. Wojewódka, *Robust device-independent randomness amplification with few devices*, arXiv:1310.4544v2 [quant-ph] (2015).
 - [8] K.M. Chung, Y. Shi & X. Wu, *Physical randomness extractors: generating random numbers with minimal assumptions*, arXiv:1402.4797 (2014).
 - [9] R. Ramanathan, F.G.S.L. Brandão, K. Horodecki, M. Horodecki, P. Horodecki & H. Wojewódka, *Randomness amplification against no-signaling adversaries using two devices*, arXiv:1504.06313 [quant-ph] (2015).
 - [10] N. Gisin, A.A. Méthot & V. Scarani, *Pseudo-telepathy: input cardinality and Bell-type inequalities*, International Journal of Quantum Information 5: 525-534 (2007).
 - [11] D.M. Greenberger, M.A. Horne & A. Zeilinger, *Bells theorem, quantum theory, and conceptions of the universe*, (Kluwer, Dordrecht), 69 (1989).
 - [12] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski & R. Ramanathan, *Free randomness amplification using bipartite chain correlations*, Phys. Rev. A 90, 032322 (2014).
 - [13] O. Gühne, G. Tóth, P. Hyllus & H.J. Briegel, *Bell inequalities for graph states*, Phys. Rev. Lett. 95, 120405 (2005).
 - [14] N.S. Jones & L. Masanes, *Interconversion of nonlocal correlations*, Phys. Rev. A 72, 052312 (2005).
 - [15] R. Ramanathan, J. Tuziemiński, M. Horodecki & P. Horodecki, *No quantum realization of extremal no-signaling boxes*, arXiv:1410.0947v2 [quant-ph] (2015).
 - [16] M. Santha & U.V. Vazirani, *Generating quasi-random sequences from slightly-random sources*, Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS'84), 434 (1984).

Appendix I

Suppose that A and B are some portions of bits from an ε -SV source of the same length $|A| = |B|$. Fix $\bar{a}, \bar{b} \in \mathcal{I}$. We assume that the probability we consider is normalized, i.e. $\sum_{a \in \mathcal{I}} P(A = a) = 1$.

Let us prove that condition

$$p_{\min} \leq P(B = \bar{b} | A = \bar{a}) \leq p_{\max} \quad (88)$$

implies that

$$\zeta_{\min} \leq P(A = \bar{a} | B = \bar{b}) \leq \zeta_{\max}, \quad (89)$$

where

$$\zeta_{\min} = \frac{p_{\min}^2}{|\mathcal{I}| p_{\max}^2} \quad \zeta_{\max} = 1 - (|\mathcal{I}| - 1) \zeta_{\min}. \quad (90)$$

Note that the definition of an ε -SV source (1) implies that

$$P(A = \bar{a}, B = \bar{b}) = P(A = \bar{a})P(B = \bar{b}|A = \bar{a}) \geq p_{\min}^2. \quad (91)$$

Let us now estimate

$$P(B = \bar{b}) = \sum_{a \in \mathcal{I}} P(A = a, B = \bar{b}) \leq p_{\max}^2 |\mathcal{I}|. \quad (92)$$

We obtain

$$P(A = \bar{a}|B = \bar{b}) = \frac{P(A = \bar{a}, B = \bar{b})}{P(B = \bar{b})} \geq \frac{p_{\min}^2}{|\mathcal{I}|p_{\max}^2}, \quad (93)$$

which proves the left side of Eq. (89). The formula for ζ_{\max} may be justified as follows

$$P(A = \bar{a}|B = \bar{b}) = 1 - \sum_{a \in \mathcal{I} \setminus \{\bar{a}\}} P(A = a|B = \bar{b}) \leq 1 - \zeta_{\min}(|\mathcal{I}| - 1). \quad (94)$$

Appendix II

Let us justify that to prove that the protocol is safe it is enough to consider boxes with either zero or one contradiction with the correlations of ideal boxes. It should be noted that using bad boxes with more than one contradiction simply decreases the probability of acceptance $P(\text{ACC})$ for the protocol, making the observed Bell value bigger. We now show that the attack with bad boxes possessing more than one contradiction can be improved by replacing these boxes with 1-contradiction boxes. There is now only one more issue that needs attention. Due to the symmetry assumption, on which our analysis is based, we need to replace boxes in such a way, that the final ensemble is symmetric. Fortunately, it can be easily achieved, as illustrated by the following example.

Suppose that any box with k contradictions on edges e_1, \dots, e_k is replaced (with probability $1/k$) by one of boxes with exactly one contradiction at one of edges e_1, \dots, e_k . Then, if we assume that all boxes with k contradictions are equally likely and are treated as described above, we will obtain the symmetric ensemble used in the main text, which justifies that constraints used in linear programming remain the same.

Appendix III

Here, we derive the constraints on the linear program Eq. (69) from Section IV.F.

Recall that $k := |l|$. Let us introduce disjoint sets T_{k+s} , $s \in \{0, \dots, m-k\}$, such that $\bigcup_{s=0}^{m-k} T_{k+s} = \mathcal{C}^1$. Every set T_{k+s} consists of sequences with $k+s$ bad boxes and belongs to the cloud \mathcal{C}^1 , which simply means that it is fixed where k detected bad boxes (with contradictions on measured edges) are. Note that

$$|T_{k+s}| = \binom{m-k}{s} (n-1)^s. \quad (95)$$

We now obtain

$$\begin{aligned} P(f = i | \mathcal{C}^1) &= \frac{P(f = i, \mathcal{C}^1)}{Q_k} = \frac{1}{Q_k} \sum_{s=0}^{m-k} P(f = i, T_{k+s}) \\ &= \frac{1}{Q_k} \sum_{s=0}^{m-k} \sum_{\text{Seq}_{k+s} \in T_{k+s}} P(f = i | \text{Seq}_{k+s}) P(\text{Seq}_{k+s}). \end{aligned} \quad (96)$$

Let us assume that i is defining the position of some detected bad box, which means that i is defining the position of a bad box in every Seq_{k+s} belonging to cloud \mathcal{C}^1 . Following the definition of the attack (see Eq. (63)), as well as Eq. (95), we obtain

$$\begin{aligned} P(f = i | \mathcal{C}^1) &= \frac{1}{Q_k} \sum_{s=0}^{m-k} \frac{1}{k+s} \sum_{\text{Seq}_{k+s} \in T_{k+s}} r_{k+s} = \frac{1}{Q_k} \sum_{s=0}^{m-k} \frac{1}{k+s} r_{k+s} |T_{k+s}| \\ &= \frac{1}{Q_k} \sum_{s=0}^{m-k} \frac{1}{k+s} r_{k+s} \binom{m-k}{s} (n-1)^s. \end{aligned} \quad (97)$$

We further obtain (due to Eqs. (68) and (62))

$$\sum_{s=0}^{m-k} \frac{1}{k+s} \binom{m-k}{s} (n-1)^s r_{k+s} \leq c_+ Q_k = \sum_{s=0}^{m-k} c_+ \binom{m-k}{s} (n-1)^s r_{k+s}, \quad (98)$$

which gives

$$\sum_{s=0}^{m-k} \left(\frac{1}{k+s} - c_+ \right) \binom{m-k}{s} (n-1)^s r_{k+s} \leq 0. \quad (99)$$

Then, according to the definition of P_j (see Eq. (61)), we have

$$\frac{1}{\binom{m}{k} n^k} \sum_{s=0}^{m-k} \left(\frac{1}{k+s} - c_+ \right) \binom{k+s}{k} \frac{(n-1)^s}{n^s} P_{k+s} \leq 0. \quad (100)$$

Finally we obtain

$$\sum_{s=0}^{m-k} \left(\frac{1}{k+s} - c_+ \right) \binom{k+s}{k} \left(\frac{n-1}{n} \right)^s P_{k+s} \leq 0. \quad (101)$$

Appendix IV

Proof of Lemma 17. To show feasibility, we need to prove that all m inequalities, given by Eq. (78), are satisfied.

Step I. Let $u \leq v$. Suppose that constraints (78) for $k = u$ and $k = v$ are equalities. Then, since $y_2 = y_3 = \dots = y_n = y_{n+2} = 0$, we have

$$\begin{aligned} u \left(\frac{n-1}{n} \right)^{u-1} \left(\frac{1}{u} - c_+ \right) y_1 + y_{m+1} &= a^u, \\ v \left(\frac{n-1}{n} \right)^{v-1} \left(\frac{1}{v} - c_+ \right) y_1 + y_{m+1} &= a^v. \end{aligned} \quad (102)$$

Suppose that

$$u = \frac{1}{c_+} \quad \text{and} \quad v = \frac{1}{c_+} + 1. \quad (103)$$

Then, after subtracting Eqs. (102), we obtain

$$y_1 = \frac{a^{1/c_+} - a^{1/c_++1}}{c_+ \left(\frac{n-1}{n}\right)^{1/c_+}} \geq 0. \quad (104)$$

Further, we verify the remaining constraints:

$$\frac{k \left(\frac{n-1}{n}\right)^{k-1} \left(\frac{1}{k} - c_+\right) a^{1/c_+} (1-a)}{c_+ \left(\frac{n-1}{n}\right)^{1/c_+}} + a^{1/c_+} \geq a^k \quad (105)$$

Step II. Take $k < \frac{1}{c_+}$ and set $0 < l = \frac{1}{c_+} - k$. Then $k \left(\frac{1}{k} - c_+\right) = 1 - kc_+ = lc_+$ and we may write Eq. (105) as follows

$$\frac{l(1-a)}{\left(\frac{n-1}{n}\right)^{l+1}} + 1 \geq a^{-l}. \quad (106)$$

To justify that this is true, we carry out the following reasoning. First, note that

$$(1-a) \leq \frac{1}{n}, \quad (107)$$

which follows from the fact that the minimal biased probability always is lower than the uniform one. Hence, we obtain

$$a^{-l} \leq \left(\frac{n-1}{n}\right)^{-(l+1)}. \quad (108)$$

Now, it is enough to prove that

$$l(1-a)a^{-l} + 1 \geq a^{-l}, \quad (109)$$

since it implies Eq. (106), due to Eq. (108). Let us write Eq. (109) as follows

$$l(1-a) + a^l - 1 \geq 0. \quad (110)$$

We have

$$\frac{d}{dl} \left(l(1-a) + a^l - 1 \right) = (1-a) + a^l \ln(a), \quad (111)$$

where \ln is the natural logarithm. Note that, since $\ln(a) < 0$, we have

$$(1-a) + a^l \ln(a) \geq (1-a) + a \ln(a). \quad (112)$$

Let us verify if

$$(1-a) + a \ln(a) \geq 0, \quad (113)$$

which is equivalent to

$$e^{\frac{1-a}{a}} \geq e^{-\ln(a)} = \frac{1}{a}. \quad (114)$$

Using the Maclaurin series expansion, we obtain

$$1 + \frac{1-a}{a} + \frac{1}{2!} \left(\frac{1-a}{a} \right)^2 + \frac{1}{3!} \left(\frac{1-a}{a} \right)^3 + \dots \geq \frac{1}{a} \quad (115)$$

which is obviously true. Hence, the value of first derivative is positive for every natural l , which means that the function on the left hand side of (110) is monotonically increasing. As a consequence, it is also non-negative, since for $l = 1$ it is equal to zero. This completes the verification of the constraints for $k < \frac{1}{c_+}$.

Step III. Now, let $k > \frac{1}{c_+} + 1$. Set $\tilde{l} + 1 = k - \frac{1}{c_+} > 0$. Analogously to the previous case, we may rewrite Eq. (105) in the following form

$$1 - a^{\tilde{l}+1} - (1-a)(\tilde{l}+1) \left(\frac{n-1}{n} \right)^{\tilde{l}} \geq 0. \quad (116)$$

Due to Eq. (107), we obtain

$$a^{\tilde{l}} \geq \left(\frac{n-1}{n} \right)^{\tilde{l}}, \quad (117)$$

which implies that to prove Eq. (116), it is enough to show that

$$1 - a^{\tilde{l}+1} - (1-a)(\tilde{l}+1)a^{\tilde{l}} \geq 0. \quad (118)$$

We obtain

$$\begin{aligned} \frac{d}{d\tilde{l}} \left(1 - a^{\tilde{l}+1} - (1-a)(\tilde{l}+1)a^{\tilde{l}} \right) &= -a^{\tilde{l}+1} \ln(a) - (1-a)a^{\tilde{l}} - (1-a)(\tilde{l}+1)a^{\tilde{l}} \ln(a) \\ &\geq a^{\tilde{l}} (-a \ln(a) - (1-a) - 2(1-a) \ln(a)). \end{aligned} \quad (119)$$

The derivative is positive, i.e.

$$-a \ln(a) - (1-a) - 2(1-a) \ln(a) \geq 0 \quad (120)$$

if

$$\ln \left(\frac{1}{a} \right) \geq \frac{1-a}{2-a}. \quad (121)$$

Note that it is enough to verify that

$$\frac{1}{a} \geq e^{1-a} \quad (122)$$

and this is easily verified by the series expansions of $\frac{1}{1-x}$ and $\exp x$. Since, we established positivity of the first derivative for every natural l , we know that the function on the left hand side of Eq. (118) is increasing. As a consequence, the function is also non-negative, which follows from the result for $l = 1$, namely that $1 - a^2 - 2(1-a)a = (1-a)^2 \geq 0$.

□